CSIRT Description for SOCA, The SOC Powered by ANECT

1. Document Information

This document contains a description of SOCA team according to RFC 2350. The document provides basic information about the team, the ways it can be contacted, describes its constituency, responsibilities and the offered services.

1.1. Date of Last Update

This is version 1.1, published on March 1st 2016.

1.2. Distribution List for Notifications

There is no distribution list for notifications about changes in this document.

1.3. Locations where this Document May Be Found

The current version of this document can always be found at http://www.soca.cz/.

2. Contact Information

2.1. Name of the Team

SOCA

2.2. Address

SOCA

ANECT a.s.

Vídeňská 204/125,

Přízřenice,

619 00 Brno

Czech Republic

2.3. Time Zone

Time-zone (relative to GMT): GMT01/GMT02 (DST)

2.4. Telephone Number

+420 271 100 986

2.5. Facsimile Number

None.

2.6. Other Telecommunication

None.

2.7. Electronic Mail Address

soca@anect.cz

2.8. Public Keys and Encryption Information

The SOCA has a PGP key. Its fingerprints can be found in chapter 2.9.

2.9. Team Members

SOCA team has following members - Aleš Mahdal, Jaroslav Třešňák, Vladimír Poprocký, Radim Koneček, Jozef Cmorej, Igor Fould, Jan Jagoš, Tomáš Jurák, Zbyněk Doupovec, Zbyněk Malý, Josef Svoboda, Radek Kulhánek and David Žák.

The SOCA team PGP key:

Team e-mail address:	soca@anect.cz
PGP KeyID:	A332507B
Key size:	2048
Key Fingerprint:	F39C 6DE3 93B0 B42D D48B A3CB 35FE 7204 A332 507B

Team member's email addresses:

UserID:	Aleš Mahdal <ales.mahdal@anect.com>
PGP KeyID:	2CE3A67B
Key size:	2048
Key Fingerprint:	6F4C 72A4 507A DB90 E776 EE76 9685 48DC 2CE3 A67B

User:	Jaroslav Třešňák <jaroslav.tresnak@anect.com>
User:	Vladimír Poprocký <vladimir.poprocky@anect.com>
User:	Radim Koneček <radim.konecek@anect.com>
User:	Jozef Cmorej <josef.cmorej@anect.com>
User:	Igor Fould <igor.fould@anect.com>
User:	Jan Jagoš <jan.jagos@anect.com>

User:	Tomáš Jurák <tomas.jurak@anect.com>
User:	Zbyněk Doupovec <zbynek.doupovec@anect.com>
User:	Zbyněk Malý <zbynek.maly@anect.com>
User:	Josef Svoboda <josef.svoboda@anect.com>
User:	Radek Kulhánek radek.kulhanek@anect.com
User:	David Žák <david.zak@anect.com>

Keys and their signatures can be found at the public keyservers. (i.e. OpenPGP at https://key.ip6.li/)

2.10. Other Information

General information about SOCA powered by ANECT can be found at:

http://www.soca.cz/, http://www.anect.cz/, http://www.anect.com

2.11. Points of Customer Contact

The preferred method for contacting SOCA team is via e-mail to soca@anect.cz. All e-mails will be handled by the responsible human – member of SOCA team or ANECT, a.s.

If you need to send any sensitive information, use PGP encryption. If it is not possible to use e-mail, or in urgent cases you can use phone number +420 271 100 986, Days/Hours of Operation: 08:00 to 18:00 Monday to Friday.

3. Charter

3.1. Mission Statement

SOCA is the SOC powered by ANECT,a.s. Main tasks of SOCA are as follows:

- To provide SOC business services
- To be a Point of Contact for clients and third parties
- To maintain relations with other CERT/CSIRT teams
- To provide security services such as:
    - Proactive services in the area of ICT security
    - Addressing ICT security incidents and coordination thereof

SOCA also handles incidents that originate in networks provided by its clients and are reported to the team by any person or institutions.

3.2. Constituency

The SOCA team constituency are networks of ANECT, a.s. and their client networks under active support service contract.

3.3. Sponsorship and/or Affiliation

Team SOCA is operated by ANECT, a.s. (http://www.anect.cz/). ANECT is a preferred ICT services provider and integrator.

3.4. Authority

SOCA is provided by ANECT,a.s. officially formed at March 2014.

All members of SOCA are employees of ANECT,a.s.

SOCA does its best for cooperation with clients and other CSIRT teams in the Czech Republic, establishes direct contacts and exchange necessary data in order to prevent and recover from ICT security incidents that affect their networks.

4. Policies

4.1. Types of Incidents and Level of Support

SOCA provides incident handling service for IP ranges assigned to ANECT, a.s. and their clients.

The level of support given by SOCA depends on the type and severity of the incident and the type of constituent, and the SOCA actual resources. Though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity.

End users of client network are expected to contact their network/system/service administrator for assistance. Only limited support can be given to the end users.

4.2. Co-operation, Interaction and Disclosure of Information

SOCA communicates and cooperates with other CSIRTs that are members of TF-CSIRT and FIRST community.

SOCA exchanges all necessary information with other CSIRTs as well as with affected network/services administrators. SOCA operates under the restrictions imposed by Czech law. It involves especially Civil code and Data Protection law.

All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted encrypted.

4.3. Communication and Authentication

For normal communication (not containing sensitive information) SOCA uses unencrypted e-mails or phone. For secure communication PGP-Encrypted communication is used.

5. Services

5.1. Incident Response

SOCA will handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Determining whether an incident is authentic
- Determining whether an incident is still relevant (if possible)
- Assessing and prioritizing the incident

5.1.2. Incident Coordination

- Determining the involved organizations
- Contacting the involved organizations to investigate the incident and take the appropriate steps
- Facilitating contact to other parties which can help resolve the incident.
- Facilitating contact with other sites which may be involved
- Facilitating contact with appropriate law enforcement officials, if necessary.

5.1.3. Incident Resolution

- Collecting the evidence of the incident.

SOCA will give advice, can established cooperation and communication between involved parties, but no physical support.

SOCA also collects statistics about reported incidents and their solving.

5.2. Proactive Activities

SOCA provides proactive services in area of warning and alerts to its clients.

SOCA provides educational services to its clients.

6. Incident Reporting Forms

There is no required format of forms for reporting the incidents to SOCA.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, SOCA assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.